	Digital Partner (DIPA) & Information Security Officer (ISO)
Reports to:	As ISO: Country director (for management reporting) CISO / ISM-T (for technical subjects) As DIPA: Directly to the LFA
Deputy:	--

1. Background

You are responsible for all matters related to digital transformation and information security within your area of responsibility. You serve as the central point of contact for management and staff on issues related to information management, IT security, and data protection — both for internal organizational aspects and local digital infrastructure.

As a Digital Partner (DIPA), you provide technical guidance to teams and ensure the quality of results in digital processes. You facilitate clear communication of objectives, conditions, and constraints, and play an active role in the development and strengthening of the organization's digital network. You support local users in the introduction and use of new digital systems, provide guidance on future technological solutions, and promote collaboration with the Head Office. In addition, you coordinate and respond to team requests, ensuring timely and efficient processing while contributing to knowledge sharing and documentation.

As an Information Security Officer (ISO), you are responsible for implementing and maintaining the Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022. This system aims to protect all valuable information processed by the organization worldwide.

In this role, you serve as the focal point for local information security management, ensuring the implementation of policies, controls, and risk assessments. You work closely with the Chief Information Security Officer (CISO) and the ISMT team, who provide global technical leadership, while disciplinary supervision is provided by the local management level.

The ISO also collaborates with IT professionals, Digital Partners (DIPA), Heads of Units, and Country Office Management, ensuring close coordination between digital processes and information security measures. To avoid conflicts of interest, the ISO role cannot be performed simultaneously with the functions of IT Professional or Head of IT Unit.

You contribute to the continuous improvement of digital and information security processes, playing an active role in advancing digital transformation and protecting the organization's information assets.

2. DIPA Requirements and Functions

- **Knowledge of processes:** Understand and monitor digitalized and documented processes within the office, identify the needs of those that remain analogue, and propose organizational improvements.
- **Compliance and information management:** Provide system-independent advice on compliant handling (according to PuR and applicable legislation) of information subject to retention, filing structures, storage, archiving, and permission management.
- **Digital advisory role:** Provide guidance at the interface with GIZ partners, in coordination with technical departments at Head Office, on the use and development of specific digital tools.
- **Process supervision:** Monitor digitalized processes and propose adjustments to existing workflows.
- **Integration and support:** Ensure that digital transformation is fully integrated into office operations and adequately resourced.
- **Capacity development:** Participate in training and capacity-building activities to strengthen digital competencies in line with GIZ guidelines.

3. ISO Requirements and Functions

- **Independence**: Reports directly to the Country Director and the LFA.
- **Organizational support:** Has access to adequate resources and budget to effectively implement information security policies.
- **Defined roles:** Roles and responsibilities are clearly established and communicated by local management.
- **Integration:** Ensure that information security is integrated into all processes (Finance, HR, Procurement, IT, etc.).
- **Internal audits**: Conduct internal audits to assess compliance with information security policies and procedures.
- **Reporting**: Submit regular reports to the Country Director, LFA and CISO/ISM-T on the state of information security.
- **Professional development**: Maintain and update competencies through continuous training and experience.
- **Awareness**: Strengthen awareness initiatives and information security programs within the office.

4. Responsibilities – DIPA and ISO

4.1 DIPA

- Act as the focal point for digital transformation.
- Promote the digitalization of processes and recommend improvements.
- Align the implementation of digital systems with GIZ global standards.
- Provide advice on data management, archiving, and information governance.
- Promote digital literacy and staff capacity development.
- Coordinate with IT, and Head Office on systems, tools, and processes.
- Ensure proper documentation and communication of digital activities and best practices.
- Contribute to integrating digital transformation across all operational and project areas.

4.2 ISO

- Serve as the focal point for information security.
- Implement, monitor, and improve the ISMS in accordance with ISO/IEC 27001:2022.
- Coordinate information security policies, standards, and risk management practices.
- Conduct internal audits and recommend corrective actions.
- Manage and report information security incidents.
- Provide regular reports to the Country Director, LFA and CISO/ISM-T.
- Collaborate with IT Professionals, DIPA, SRMO, and project teams.
- Promote awareness and training campaigns on information security.
- Ensure the confidentiality, integrity, and availability of information.
- Support certification processes and continuous improvement.

5. Tasks

In addition to the responsibilities mentioned above, the ISO–DIPA role includes the following tasks:

5.1 ISO

- Implement, coordinate, and continuously improve the local ISMS.
- Coordinate, develop, and review security policies and related sub-concepts.
- Plan and coordinate the implementation of information security measures with HQ-ISMT, IT, Data Protection, and SRMO.
- Monitor the effectiveness of the security program and recommend improvements.
- Support incident management, including assessment, communication, and follow-up.
- Advise and report to management on ISMS performance.
- Develop internal audit plans and support external audits.
- Serve as the contact point for all non-conformities.

5.2 DIPA

- Promote knowledge transfer through training and workshops.
- Stay updated on digital solutions and coordinate with DIGITS/Global IT Services.
- Disseminate best practices and key aspects of digital transformation.
- Act as a multiplier for digital tools and solutions (e.g., LSS S4GIZ).
- Create content for multi-channel communication and new staff onboarding.
- Advise users on tools, document management systems (M365 and Sharepoint), and compliance.
- Serve as the first point of contact for basic topics related to classification, labelling, and data protection.
- Participate actively in communication channels with Head Office regarding data protection.
- Translate DIGITS recommendations into clear materials for end users.
- The DIPA reports only to the LFA

Perform additional tasks assigned by the supervisor, in accordance with operational and organizational needs.

6. Qualifications

The position holder should have:

- At least 5 years of professional experience in an international organization with more than 1,000 employees, familiar with organizational structures and processes.
- A university degree in information systems, computer science, management, or a related field.
- Strong knowledge and experience in information security, including ISO/IEC 27001:2022, risk management, vulnerability management, and auditing.
- Experience in digitalization, document management, and data protection processes.
- Excellent communication, advisory, and teamwork skills.
- High level of integrity, discretion, and analytical thinking.
- A proactive attitude, results orientation, and commitment to continuous improvement.
- Fluency in English (C1), optional German.

In line with our inclusion policy, gender strategy, and commitment to diversity, we value the multiplicity of perspectives and the enrichment that diverse teams bring. At GIZ Colombia, we actively encourage the participation of women, LGBTQ+ individuals, people with disabilities, and people of diverse ethnic backgrounds in all stages of the selection and hiring processes, and we invite them to submit their applications.

Interested candidates are invited to send their resume in Spanish, along with a cover letter and salary expectations, to HR-GIZColombia@giz.de by January 19, 2026.